United States Department of State

Privacy Impact Assessment

U.S. Speaker and Specialist Program

(TRKR II – ITAB Number 5189)

Bureau of Administration

1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld Bureau of Administration Global Information Services Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: August 27, 2013

(b) Name of system: Tracker II

(c) System acronym: TRKR II

(d) IT Asset Baseline (ITAB) number: 5189

(e) System description (Briefly describe scope, purpose, and major functions):

Tracker II is a central data repository for the U.S. Speaker and Specialist Program managed by the Bureau of International Information Programs (IIP). Each year IIP's Worldwide Speaker Program organizes around 650 traveling speakers, and virtual interactive outreach programs in cooperation with posts worldwide. All U.S. Speaker and Specialist grantees must be U.S. citizens. Major components of this program include: traveling speakers and virtual Interactive Electronic Speaker Programs.

- Traveling Speakers — Bringing an expert from the United States to speak to foreign audiences is a compelling way for posts to deliver messages about American policy, society, institutions or culture. IIP Programs send hundreds of speakers each year to posts around the world.
- Virtual Interactive Electronic Speaker Programs— IIP can help posts to reach out to audiences with live interactive video conferences with key experts. Virtual webchats and podcasts are also some of the ways IIP's Speaker Program is expanding our dialog with foreign opinion leaders and publics, both geographically and over time.

The Tracker II System stores bios and curricula vitae on participating and potential speaker and specialists. It tracks the funding, authorization, significant communications and evaluations for: traveling and virtual speakers, video conferences, electronic telepress, and conferences. The system is also used to initiate and produce individual grants, to provide a business workflow for Speaker projects and to monitor expenditures for U.S. Speaker and Specialist Program services requested by DoS field posts throughout the world. Tracker II is a closed accounting system, with manual re-entries into the U.S. Department of State's Global Financial Management System (GFMS).

(f) Reason for performing PIA:

☐ New system

☒ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

(g) Explanation of modification (if applicable):

The Tracker system is retired and replaced with the Tracker II system.

This change constitutes a significant change.

(h) Date of previous PIA (if applicable): August 2009

3. Characterization of the Information

The system:

☐ does NOT contain Personally Identifiable Information.

☒ does contain Personally Identifiable Information.

a. What elements of Personally Identifiable Information (PII) are collected and maintained by the system? What are the sources of the information?

The following are elements of PII collected and maintained in Tracker II on individuals who are participating as speakers or presenters in the International Information Programs (IIP) Speaker and Specialist Program:

- Name of Speaker/Specialist
- Date and place of birth
- Gender
- Address
- Telephone, cell, fax numbers
- Social Security number
- Passport number
- Visa numbers
- Education
- Financial transactions

  Tracker maintains the individual's social security number and payment amount and includes them on the generated Public Voucher for Purchases and Services Other than Personal (Standard Form 1034A). The form is used internally to authorize and verify payment to the speaker.

  Outside the system, the Automated Clearing House (ACH) Vendor / Misc Payment Enrollment Form (SF3881) is completed with the speaker's contact information and social security number, as well as the their bank routing number, account number, contact information.

b. How is the information collected?

Data is collected directly from the record subjects. Additional data may be collected from publicly available information on the internet and through media reports. The U.S. Speaker and Specialist Program staff use the internet to obtain bios, read papers,

interviews, and articles written by potential speakers, and to look at lectures on YouTube.

Banking and other PII is obtained over the phone by the U.S. Speaker and Specialist Program staff, or the grantee faxes/emails a completed questionnaire back to the International Information Programs (IIP) program officer.

All collected data is manually entered by the International Information Programs staff.

c. Why is the information collected and maintained?

For Tracker II, the information is collected and maintained to recruit speakers, process individual grants, schedule travel and engagements, manage financial accounting, make payments to speakers as compensation for their time, and summarize results for government reporting requirements.

d. How will the information be checked for accuracy?

Information collected directly from the record subject is presumed to be accurate. The contact information about an individual is collected from Department of State records and interviews with the subject individual.

If the subject's social security number and banking information do not match, payment cannot be made to the individual.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

- 5 U.S.C. 301 (Management of the Department of State);
- 22 U.S.C. 1431 et seq. (Smith-Mundt);
- United States Information and Educational Exchange Act of 1948, as amended;
- 22 U.S.C. 2451-58 Fulbright-Hays Mutual Educational and Cultural Exchange Act of 1961, as amended;
- 22 U.S.C. 2651 a (Organization of the Department of State); and
- 22 U.S.C. 3921 (Management of the Foreign Service).

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

A potential privacy risk involves unauthorized access to a Speaker's banking information for malicious usage. This risk is mitigated by hosting the Tracker II system and data only on the Department of State's intranet and not making that system and data available via the internet. This hosting restriction lessens the PII data exposure to only Department employees who must first be authorized to access the Department's intranet and then only to those whose role and need-to-know require them to be granted access by the system owner.

For Tracker II, information collected and maintained is the minimum amount of information necessary to fulfill IIP's statutorily mandated U.S. Speaker and Specialist Program. The information is required to award individual grants, make payments to individuals, draft itineraries, plan and program Speaker activities, manage financial accounts, and obtain required visas.

Social security information and other sensitive elements of PII are collected in order to fulfill payment and coordinate with the record subjects' financial institution of choice, and

obtain any necessary visas or travel documents. Data is checked for accuracy as submitted by the record subject and is verified against Department Records where appropriate.

4. Uses of the Information

a. Describe all uses of the information.

For Tracker II, the information is required to award individual grants, make payments to individuals, draft itineraries, plan and program Speaker activities, manage financial accounts, and obtain required visas.

Within the system, the individual record of the Speaker can be retrieved by their name in actual practice. There is no retrieval of records by the Speaker's social security number, passport number or visa number.

b. What types of methods are used to analyze the data? What new information may be produced?

The data in Tracker II is not used for analytical purposes. No new information may be produced, except high-level statistics for program reporting purposes sent to the White House and Congress as required.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

Tracker II uses information from the U.S. Department of State Visa and Passport Office for visa requirements. The U.S. Office of Personnel Management provides per diem and travel rates.

d. Are contractors involved in the uses of the PII?

Contractors are involved with the operational maintenance of the system. Contractors use the data in Tracker II consistent with the statutory purposes, and do not produce any additional data. Privacy Act contract clauses are inserted in their contracts and other regulatory measures are addressed. Rules of Behavior have been established and training regarding the handling of PII under the Privacy Act of 1974 is conducted.

Contractors are employed by the U.S. Department of State within the Bureau of International Information Programs (IIP) as members of staff to support Bureau programs. All contractors, whether technical or direct program support, must pass a government background check prior to having system access. Annual, recurring security training is practiced and conducted through Diplomatic Security.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

Data collected and maintained by Tracker II is only used for purposes related to the IIP Speaker and Specialist Program. The information is not analyzed or disseminated for any other purpose. Tracker II does not provide flexibility of features that might initiate a functional vulnerability creep or threat.

Authorized employees are assigned level-of-access roles based on their job functions. Roles limit the update and printing capabilities to those deemed necessary for specified job functions.

Because personally identifiable information is collected and maintained by Tracker II, appropriate management, technical and operation security controls are in place to ensure the confidentiality and integrity of the data. Access is available only to authorized Department of State employees performing sanctioned duties. Users must pass a government background check prior to having system access. Annual, recurring security training is practiced and conducted through Diplomatic Security. Access to computerized files is password-protected. The computerized files are available only on the Department of State intranet

5. Retention

a. How long is information retained?

Records in Tracker II will be maintained until they become inactive, at which time they will be destroyed or retired in accordance with published record schedules of the Department of State and as approved by the National Archives and Records Administration. The specific schedules that apply to records in Tracker II are in Chapter 37, Section 10, items A-37-01-03 through A-37-01-03c and are found at: http://infoaccess.state.gov/recordsmgt/DispSchSection.asp?cat=records&RMH=A&Chapter=37&Section=010

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

A potential risk may occur when a programmed Speaker has out-dated information in the Tracker II system. This risk is mitigated through the requirement that Program Officers must validate with the Speaker all personal information for correctness and completeness prior to their next speaking engagement.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

In Tracker II, information is shared with U.S. Department of State's overseas Posts that request the Speaker Program in order for them to prepare for the program. Data shared is the individual's name, biography, travel itinerary and email address. No passport, visa or social security numbers are shared, except through the Department of State e-Country Clearance system.

If a Country Clearance is requested, it comes from the Speaker and Specialist Program staff in Washington, DC to the Post to ensure that the Speaker has permission to enter the country under Embassy auspices. This communication is outside and separate from the Tracker System. The Speaker staff enters the request in eCountry Clearance, a separate system on the Department of State's intranet.

The U.S. Speaker and Specialist Program staff completes the Automated Clearing House Vendor / Miscellaneous Payment Enrollment Form (ACH) with the speaker's contact and banking information and fax or email via Department of State's intranet, the

form to the Global Financial Services Center (GFSC) in Charleston, SC facility. The original form is kept by Speaker Program staff for 3 years and then shredded on-site. GFSC provides a discrete vendor code for each Speaker, which is in turn entered into Tracker II.

This ACH form is not generated from Tracker II. The Charleston Center processes the form and initiates payment to the speaker's account by entering the required information into the Department's Global Financial Management System (GFMS).

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

The information shared with the Financial Payment Center is faxed from the U.S. Department of State's equipment and phone lines. After staff receives the returned form with verification of payment, the form is shredded.

Other information is transmitted using the Department of State's email system.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

Tracker II is internal to the Department of State. The public does not have direct access to any of the systems.

A potential risk to privacy from internal sharing arises when employees assume they are by default, authorized to access any privacy information they want if the hosting agency is authorized to process the information. However, access to privacy information is restricted not only to the agency managing the U.S. Speaker and Specialist Program, but also to only those employees whose role is explicitly granted authorization to access and, if necessary, process privacy information.

When shared within the Department, all information is still used in accordance with Tracker II's stated authority and purpose. Risks to privacy are mitigated by granting explicit access only to authorized persons within the Department.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

In the **Tracker II** system, the information is shared with Atlas Visa Services, Inc, to process visas required by Speakers for their overseas travel. Data shared is the individual's name, place and date of birth, address, passport number and date of issuance, and travel itinerary. The individual's social security number is not shared. The Speaker's name and date of birth are also shared with the Department of State's travel contractor, CWT-SatoTravel, in order to make travel reservations.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

Information is shared with Atlas Visa Services, Inc. and CWT-SatoTravel via phone calls, emails and faxes. All communication is transmitted via secure U.S. Department of State communication channels.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

By sharing privacy information externally, one runs the potential risk of having less control over the environment than if privacy information were restricted to a limited intranet and within defined physical boundaries. By sharing privacy information externally, the external entity may accidentally or intentionally share the information with others within their business environment who are not explicitly granted authorization to access the information.

For Tracker II, risks to privacy are mitigated by limited access to and release of personal information on a need-to-know basis to Atlas Visa Services, Inc and CWT SatoTravel.. As vendors of the United States government, Atlas Visa Services, Inc, CWT SatoTravel and employees maintain a government security clearance. Information is only released on a need-to-know basis to Atlas Visa Services, Inc and CWT SatoTravel under a statutory or other lawful authority to maintain such information. The information is used in accordance with the statutory authority and purpose.

8. Notice

The system:

☒ contains information covered by the Privacy Act.

Provide number and name of each applicable system of records.

(visit *www.state.gov/m/a/ips/c25533.htm* for list of all published systems):

STATE-65 Speaker/Specialist Program Records

STATE-40 Employee Contact Records

☐ does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

A Privacy Act Statement is available for those individuals that provide this information by form, and notice is also given through System of Records Notices State-65 and State-40.

b. Do individuals have the opportunity and/or right to decline to provide information?

The individual may decline to provide the required information; however, for the IIP Speaker and Specialist Program, such actions may prevent individuals from participating in that Program.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

Conditional consent is not applicable to the official purpose of Tracker II.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

For the IIP Speaker and Specialist Program, notice is provided to individuals as part of the Grant Award Letter, and a Privacy Act Statement is available on all forms. Furthermore, notification is provided to the public via System of Records Notices State-65 and State-40.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

Individuals who wish to gain access to or amend records pertaining to themselves should write to the Director, Office of Information Programs and Services; Department of State; SA-2; 515 22nd Street NW; Washington, DC 20522-6001. The individual must specify that they wish the Cultural Property Advisory Committee Records to be checked. At a minimum, the individual should include: Name; date and place of birth; social security number; current mailing address and zip code; signature; a brief description of the circumstances that caused the creation of the record, and the approximate dates which give the individual cause to believe that the Office of International Information Programs has records pertaining to them.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

A privacy risk associated with notification and redress can potentially occur when a Speaker has a change in his or her contact or banking information and does not communicate that change to the Department's U.S. Speaker and Specialist staff. This can potentially cause a Speaker's Visa to be rejected or the Speaker to not be paid per the individual grant agreement.

To mitigate these risks, Speaker Program Officers and Coordinators keep the Speaker informed from the beginning of communications that the collected information provided about and by the Speaker is maintained in the U.S. Speakers and Specialist Program system called Tracker II. The staff also reminds the Speaker that if the Speaker's provided information should change during the course of the engagement, that the Speaker must contact the respective Program staff to update the information.

Speakers can contact their respective Program Officer or the Bureau of International Information Programs to ask what is recorded about them and request that information be amended if they believe it to be incorrect. The notice is reasonable and adequate in relationship to the system's purpose and use.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

For the Tracker II system, the system functional administrators determine, on a case by case basis, who in the respective office staff is authorized to access the system and at what level. The level of access and capabilities permitted are restricted by the role assigned to each individual user. Some users are granted read-only access if they have no need to update system records. The separation of roles with different access privileges is in accordance with NIST Special Publication 800-53.

All authorized staff using the system must comply with the Department of State's general "appropriate use policy for information technology". Rules of behavior and consequences, and system use notifications are in accordance with the Privacy Act (subsection e[9]) and OMB Circular A-130, Appendix III.

The security controls in the system are reviewed when significant modifications are made to the system, but at least every three years.

Access to Tracker II is restricted to Department of State personnel that are approved to use the Department's intranet. Only personnel with an approved ID and password can make select updates to the respective system. There is no placement of personally identifiable information (PII) on portable computers. Authorized system users who telecommute can only access the system through the Department of State's secure access using the Global OpenNet remote access software package with two-factor authentication where one of the factors is provided by a RSA soft/hard token with a use-once password.

Department of State system users must pass a government background check prior to having system access. At a minimum, they must possess a security clearance level of confidential, with secret preferred. Annual, recurring security training is practiced and conducted through Diplomatic Security.

Authorized user login identifiers are appended to any system records created or updated, along with the date and time of the record creation or change. This allows administrators to identify the source of any incorrect or incomplete data as recorded in the system.

Contractors authorized to access the system are governed by contracts identifying rules of behavior for Department of State systems and security. Contracts are reviewed upon renewal by management and contract personnel expert in such matters.

b. What privacy orientation or training for the system is provided authorized users?

Annual, recurring security training is practiced and conducted through the Bureau of Diplomatic Security. Additionally, all Department direct hires and locally employed staff (LES) must pass PA-459, a course entitled Protecting Personally Identifiable Information.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Several steps are taken to reduce residual risk related to system and information access. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly terminated. Additionally, the system audit trails that are automatically generated are regularly

analyzed and reviewed to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a particular user performed--or attempted to perform--on an information system.)

The assessment and authorization process independently verifies and validates the application system security controls. Administrative procedures, including independent security investigations of Department applicants and assignment of unique system access rights to individuals, limit access to the system.

There is little residual risk related to access, in particular because the system is available only on a Department of State intranet and there is no direct electronic transfer of data between Tracker II systems and external organizations or individuals.

11. Technologies

a. What technologies are used in the system that involve privacy risk?

No technology used in Tracker II elevates the privacy risk in the system.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

No technology used in Tracker II elevates the privacy risk in the system.

12. Security

What is the security assessment and authorization (A&A) status of the system?

As a component system to the International Information Programs, Program Management and Outreach System, Tracker II was granted Full Accreditation at the Sensitive-But-Unclassified (SBU) level August 31, 2010. The authorization is valid for up to 36 months. This Accreditation expires on August 31, 2013, or upon significant change to the system, application, or environment. IIP-PMOS is currently going through recertification and anticipates it to receive a provisional ATO until the ongoing recertification is completed and a full ATO can be granted before the end of 2013.